POINT OF VIEW

Complexities in Deploying Zero Trust in Operational Technology

Taking Operational and Cybersecurity Risks into Account

Executive Summary

Corporations and CISOs are improving security by implementing zero trust in their IT networks. But, less consideration has been given to zero trust in operational technology (OT) environments because of concerns related to legacy equipment, lack of security controls, operational or production concerns, and safety constraints. Although most of these concerns are valid, collaboration and discussion between IT and OT security teams about actual barriers and boundaries can unlock apprehensions so that organizations can include OT networks in their comprehensive zero-trust security strategies.

Understanding Risks to OT Networks

Security for OT networks and devices can no longer be ignored. In the past, industrial facilities, critical infrastructure, and the associated OT networks were not designed for the modern connected world. Most OT networks were "air-gapped" from IT networks, and network and OT device security were not requirements or even considerations. Fast forward to today, and the rapid adoption of the Internet of Things, Industrial Internet of Things, and the digitization of manufacturing require connectivity to optimize production and operations and to access technology such as the cloud and artificial intelligence.

The 2023 State of Operational Technology and Cybersecurity Report found that 32% of respondents indicated both IT and OT systems were impacted by cyberattacks, an increase from 21% in 2022.[1]

Although the benefits of IT/OT network convergence are clear, it incurs additional risks. As factories are connected, improper or lacking security can expose critical infrastructure, equipment, and personnel to new cyberthreats. Because of recent industrial attacks, the impact of malicious cyberattacks that directly or indirectly affect production or public safety is better understood by bad actors. They are increasing ransoms to include production impacts and focusing more on high-value OT targets.

Balancing Operational and Cybersecurity Risks

Implementing zero trust in OT environments may face challenges and resistance within the organization. Production, operational, and safety concerns are valid, yet there are equal concerns regarding security in terms of production risks and access control. These two sets of concerns do not need to oppose each other. They should be discussed with the understanding that implementing zero trust in OT can benefit everyone. The need for external support from OEMs, system integrators, and internal employee access must also be considered to adequately support operations and security in the face of continuing cybersecurity skills shortages.

Concerns about production interruption, stoppage, and reliability also must be addressed. Since problems can be caused by improper operator error, implementing zero trust in OT restricts access to people and systems, which can avoid inadvertent production loss. When zero trust is implemented, security increases and production risk mitigated.

75% of manufacturers rank cybersecurity as a top five business risk.[2]

Examining Strategic Objectives

Once goals and objectives for implementing zero trust in OT have been established, a best practice is to gradually introduce facets of zero trust instead of broadly introducing numerous zero trust solutions simultaneously. Because of the need for remote support and access, security teams often have already implemented a virtual private network (VPN) to grant access. The next step is to enhance the security of the connection by leveraging secure remote access (SRA) or privileged access management (PAM) along with multi-factor authentication (MFA). This migration from VPN to SRA/PAM and MFA broadens the zero trust in OT methodology. An additional consideration is to evaluate IT and OT zero-trust solutions together. Determine if you need two vendors or if a single vendor can support both IT and OT. Asking strategic questions about vendor consolidation can improve efficiency by using a common zero-trust solution set.

Mitigating Production and Cyber Risks

Initiating or expanding zero-trust security principles in OT environments comes with unique challenges and production and public infrastructure risks that are visible at the executive and public levels. Increasing cybersecurity using zero-trust principles helps better protect OT networks from adversaries looking to attack and ransom high-value OT assets. After careful consideration among diverse operational and security teams, implementation of zero trust in OT can lead to mutual benefits and mitigate both production and cyber risks.

[1] 2023 State of Operational Technology and Cybersecurity Report, Fortinet, May 24, 2023.

[2] "Advancing Digital Transformation in a Time of Unprecedented Cybersecurity Risk," Fortinet and Manufacturers Alliance, 2023.

FORTINET

www.fortinet.com

April 9, 2024 8:43 PM

2638209-0-0-EN